TITLE OF THE INVENTION

コンテンツ利用管理システム、コンテンツ利用管理方法及びクライアント機器（CONTENT USE MANAGEMENT SYSTEM, CONTENT USE MANAGEMENT METHOD, AND CLIENT DEVICE）

BACKGROUND OF THE INVENTION

(1) Field of the Invention

本発明は、音楽データ及び映像データ等のデジタルコンテンツを配信するサーバとクライアント機器とを備えるコンテンツ利用管理システム、コンテンツ利用管理方法及びクライアント機器に関する。

(2) Description of the Prior Art

ネットワークを介したコンテンツ配信システムにおいて、配信するコンテンツは暗号化され、暗号化コンテンツと暗号化したコンテンツの復号鍵（以下、コンテンツ鍵と略記する）がユーザ端末へ配信される。

コンテンツ鍵の配信方式には次の２種類がある。コンテンツの利用を要求してきたクライアント機器にのみ一対一でコンテンツ鍵を配信するユニキャスト配信と、コンテンツの利用を要求していないクライアント機器にも一斉にコンテンツ鍵を配信するマルチキャスト配信である。従来は、１つのコンテンツ配信システムにおいては、コンテンツの種別に関わらずコンテンツ鍵は同一の配信方式にて配信されている。

以上のことは文献「特開平１１－３１２１７５号公報」に記載されている。

しかしながら、コンテンツ鍵を配信するクライアントの数はコンテンツによって異なる。コンテンツを利用するクライアント機器が多い場合、ユニキャスト配信では各クライアント機器と通信を行った上でコンテンツ鍵を配信するので、ユニキャスト配信よりもマルチキャスト配信を行う方がサーバの負荷が低い。一方、ユニキャスト配信では、どのクライアント機器にどのコンテンツ鍵を配信したかといった情報をログに残すことができるので、著作権を保護する上でマルチキャスト配信よりも高い安全性を確保することができる。従来技術では、コンテンツに関わらずコンテンツ鍵をいずれか一方の配信方式で配信しているので、コンテンツによってはマルチキャスト配信方式でコンテンツ鍵を配信した方がサーバ負荷を軽減できるにもかかわ

らず、サーバ負荷が高い方式で配信されている。また、コンテンツによってはより高い安全性が望まれるにもかかわらず、安全性の低い方式で配信されている。

SUMMARY OF THE INVENTION

そこで、本発明では、上記問題点に鑑み、コンテンツに応じて選択的に、システム内の通信負荷を軽減し又はセキュリティを確保してコンテンツ復号鍵を配信できるコンテンツ利用管理システムを提供することを目的とする。

本発明におけるコンテンツ利用管理システムは、クライアント機器におけるコンテンツの利用を制御するための利用制御データを、ネットワークを介して配信するコンテンツ利用管理システムであって、前記利用制御データを、クライアント機器へ複数の異なる配信方式により配信する１以上の配信サーバと、コンテンツの属性に応じて、各コンテンツの利用制御データを、いずれの配信方式で配信するかを決定する配信管理サーバとを備え、前記配信サーバのいずれか１つは、決定された配信方式による前記利用制御データの配信を実行することを特徴とする。

以上のように、本発明によれば、コンテンツ利用管理システムは複数の異なる配信方式で利用制御データを配信する配信サーバを備え、コンテンツに応じて、利用制御データの配信方式を切り替えることにより、配信サーバの負荷およびセキュリティ確保の観点から最適な配信方式で利用制御データを配信することが可能になる。

また、前記コンテンツの属性は、コンテンツの圧縮フォーマットであって、前記配信管理サーバは、各コンテンツの圧縮フォーマットに応じて、前記利用制御データの配信方式を決定するとしてもよい。

また、前記コンテンツの属性は、コンテンツを提供するコンテンツ提供者であって、前記配信管理サーバは、各コンテンツのコンテンツ提供者に応じて、前記利用制御データの配信方式を決定するとしてもよい。

また、前記コンテンツの属性は、コンテンツの圧縮率であって、前記配信管理サーバは、各コンテンツの圧縮率に応じて、前記利用制御データの配信方式を決定するとしてもよい。

また、前記コンテンツの属性は、コンテンツの利用条件であって、前記配

信管理サーバは、各コンテンツの利用条件に応じて、前記利用制御データの配信方式を決定するとしてもよい。

また、前記１以上の配信サーバは、クライアント機器からの要求に応じてデータを配信するユニキャスト配信方式により、前記利用制御データを配信するユニキャスト配信手段と、所定の配信時刻に複数のクライアント機器に対して一斉にデータを配信するマルチキャスト配信方式により、前記利用制御データを配信するマルチキャスト配信手段との少なくとも１つを備えるとしてもよい。

また、前記配信管理サーバは、前記配信方式を決定するためのルールを示した配信方式決定ルールを保持する配信方式決定ルール保持手段と、前記コンテンツの属性に対応する前記配信方式決定ルールを参照し、前記配信方式決定ルールに従って前記配信方式を決定する配信方式決定手段とを備えるとしてもよい。

また、前記ユニキャスト配信手段を備える配信サーバは、さらに、各クライアント機器との通信により、前記クライアント機器があらかじめ登録されたクライアント機器であることを確認できた場合、前記クライアント機器を正当なユーザであると認める認証手段を備え、前記ユニキャスト配信手段は、前記認証手段により、正当なユーザであると認められたクライアント機器に対してのみ前記利用制御データを配信するとしてもよい。

また、前記利用制御データは、暗号化されたコンテンツを復号するための復号鍵を含み、前記クライアント機器は、各コンテンツに対応する利用制御データを、いずれかの前記配信サーバから取得する利用制御データ取得手段と、取得された前記利用制御データから前記復号鍵を抽出し、抽出された復号鍵を用いて前記利用制御データに対応するコンテンツを復号する復号手段と、復号された前記コンテンツを再生する再生手段とを備えるとしてもよい。

また、前記利用制御データは、さらに、コンテンツを利用するための条件を示した利用条件を含み、前記クライアント機器は、さらに、取得された前記利用制御データから前記利用条件を抽出し、抽出された利用条件が満足される範囲内で前記再生が行われるよう前記再生手段を制御する再生制御手段を備えるとしてもよい。

さらに、本発明におけるコンテンツ利用管理方法は、クライアント機器に

おけるコンテンツの利用を制御するための利用制御データを、ネットワークを介して配信するサーバのためのコンテンツ利用管理方法であって、コンテンツの属性に応じて、各コンテンツの利用制御データを、いずれの配信方式で配信するかを決定する配信方式決定ステップと、複数の相異なる配信方式のうち、決定された配信方式で前記利用制御データを配信する配信ステップとを含むことを特徴とする。

また、前記コンテンツ利用管理方法では、前記配信方式を決定するためのルールを示した配信方式決定ルールをあらかじめ保持し、前記配信方式決定ステップでは、前記コンテンツの属性に対応する前記配信方式決定ルールを参照し、前記配信方式決定ルールに従って前記配信方式を決定するとしてもよい。

さらに、本発明におけるクライアント機器は、クライアント機器におけるコンテンツの利用を制御するための利用制御データを、複数の異なる配信方式により、ネットワークを介して配信するコンテンツ利用管理システムにおけるクライアント機器であって、コンテンツを配信するコンテンツサーバに対し、コンテンツの配信を要求してコンテンツを取得するコンテンツ要求手段と、前記コンテンツサーバからの前記コンテンツの取得の成否に応じて、要求した前記コンテンツに対応する利用制御データの配信方式を判定する配信方式判定手段と、判定された配信方式で前記利用制御データを配信する配信サーバから、前記利用制御データを取得する利用制御データ取得手段とを備えることを特徴とする。以上のように、本発明によれば、マルチキャスト配信される利用制御データがコンテンツに重畳されて配信される場合においても、クライアント機器側で利用制御データの配信方式を判定することができる。これにより、コンテンツに応じて利用制御データの配信方式が異なる場合であっても、問題なく利用制御データを取得し、コンテンツを利用することができる。

また、クライアント機器におけるコンテンツの利用を制御するための利用制御データを、複数の異なる配信方式により、ネットワークを介して配信するコンテンツ利用管理システムにおけるクライアント機器であって、コンテンツを配信するコンテンツサーバから、各コンテンツに対応する利用制御データの配信方式を示す情報を含んだコンテンツを取得するコンテンツ取得手段と、取得された前記コンテンツから前記配信方式を示した情報を抽出し、

抽出された前記情報に基づいて、前記コンテンツに対応する利用制御データの配信方式を識別する配信方式識別手段と、識別された配信方式で前記利用制御データを配信する配信サーバから、前記利用制御データを取得する利用制御データ取得手段とを備えるとしてもよい。従って、利用制御データの配信方式を示す情報がコンテンツに重畳されている場合においても、クライアント機器側で利用制御データの配信方式を識別することができる。これにより、コンテンツに応じて利用制御データの配信方式が異なる場合であっても、問題なく利用制御データを取得し、コンテンツを利用することができる。

また、クライアント機器におけるコンテンツの利用を制御するための利用制御データを、複数の異なる配信方式により、ネットワークを介して配信するコンテンツ利用管理システムにおけるクライアント機器であって、前記利用制御データの配信方式を決定するサーバから、各利用制御データの配信方式を示す情報を取得する方式情報取得手段と、前記配信方式を示す情報に基づいて、前記コンテンツに対応する利用制御データの配信方式を識別する配信方式識別手段と、識別された配信方式で前記利用制御データを配信する配信サーバから、前記利用制御データを取得する利用制御データ取得手段とを備えるとしてもよい。以上のように、利用制御データの配信方式を決定するサーバから、各利用制御データの配信方式を示す情報を取得する場合においても、クライアント機器側で利用制御データの配信方式を識別することができる。これにより、コンテンツに応じて利用制御データの配信方式が異なる場合であっても、問題なく利用制御データを取得し、コンテンツを利用することができる。

なお、本発明は、このようなコンテンツ利用管理システムとして実現することができるだけでなく、これらのコンテンツ利用管理システムを構成するコンテンツ配信管理サーバ、ユーザ管理サーバ、暗号化コンテンツ配信サーバ、ユニキャスト配信サーバ、マルチキャスト配信サーバ及びクライアント機器などの単体として実現したり、これらのコンテンツ利用管理システムにおける特徴的な動作をステップとするコンテンツ利用管理方法として実現したり、その特徴的な動作をパーソナルコンピュータ等の汎用のコンピュータに実行させて機能させるプログラムとして実現することもできる。そして、そのプログラムは、ＣＤ－ＲＯＭ等のコンピュータ読み取り可能な記録媒体やインターネット等の伝送媒体を介して頒布することができるのは言うま

でもない。

BRIEF DESCRIPTION OF THE DRAWINGS

図１は、本発明におけるコンテンツ配信サービスシステムの概念図である。

図２は、ユーザ管理ＤＢの管理データの一例を示す図である。

図３は、コンテンツホルダ管理ＤＢの管理データの一例を示す図である。

図４は、コンテンツ配信方式管理ＤＢの管理データの一例を示す図である。

図５（ａ）は、配信スケジュールＤＢで保持される配信スケジュール表の更新前の一例を示す図である。

図５（ｂ）は、配信スケジュールＤＢで保持される配信スケジュール表の更新後の一例を示す図である。

図６は、配信データ管理ＤＢの管理データの一例を示す図である。

図７は、暗号化コンテンツ管理ＤＢの管理データの一例を示す図である。

図８（ａ）は、図１に示したユニキャストコンテンツＤＢに格納される暗号化コンテンツのデータ構造を示す図である。

図８（ｂ）は、図１に示したマルチキャストコンテンツＤＢに格納される暗号化コンテンツのデータ構造を示す図である。

図９は、コンテンツホルダによるコンテンツの登録のフローチャートである。

図１０は、コンテンツのメタデータの一例を示す図である。

図１１は、コンテンツ鍵・利用条件の配信方式の決定方法のフローチャートである。

図１２（ａ）は、パラメータがコンテンツの圧縮フォーマットである場合の配信方式決定ルールＤＢの管理データの一例を示す図である。

図１２（ｂ）は、パラメータがコンテンツホルダＩＤである場合の配信方式決定ルールＤＢの管理データの一例を示す図である。

図１２（ｃ）は、パラメータがＣＢＲおよびＶＢＲの平均レートである場合の配信方式決定ルールＤＢの管理データの一例を示す図である。

図１２（ｄ）は、パラメータがコンテンツ利用条件である場合の配信方式決定ルールＤＢの管理データの一例を示す図である。

図１３は、ユーザ登録のフローチャートである。

図１４は、コンテンツ利用までのフローチャートである。

図１５は、クライアント機器の構成を示す機能ブロック図である。

図１６は、クライアント機器での再生処理を示すフローチャートである。

図１７は、コンテンツ鍵の配信方式を示す情報が暗号化コンテンツデータに重畳されている場合におけるコンテンツのデータ構造の一例を示す図である。

DESCRIPTION OF THE PREFERRED EMBODIMENT(S)

以下、本発明の実施の形態について、図１から図１７を参照して説明する。

図１に実施の形態に係る動画コンテンツ配信サービスシステムの概念図を示す。クライアント機器１１０は、インターネットなどの通信路１３０を通じて、コンテンツ配信管理サーバ１２１、マルチキャスト配信サーバ１２２、ユニキャスト配信サーバ１２３、暗号化コンテンツ配信サーバ１２４、ユーザ管理サーバ１２０に接続されている。また、コンテンツ配信管理サーバ１２１は、インターネットなどの通信路１３０を通じて、マルチキャスト配信サーバ１２２、ユニキャスト配信サーバ１２３、暗号化コンテンツ配信サーバ１２４、ユーザ管理サーバ１２０に接続されている。また、マルチキャスト配信サーバ１２２、ユニキャスト配信サーバ１２３をまとめてコンテンツ鍵配信サーバと呼ぶ。

本システムを用いた動画コンテンツ配信サービスは、予めユーザ登録をしたユーザがクライアント機器１１０を利用してインターネットなどの通信路１３０を介して動画コンテンツを再生できる環境を提供するサービスである。

ユーザに配信されるコンテンツは、コンテンツホルダにより暗号化され、一旦、コンテンツ配信管理サーバ１２１を経由して、マルチキャスト配信サーバ１２２又は暗号化コンテンツ配信サーバ１２４に登録される。

ユーザは暗号化コンテンツをマルチキャスト配信サーバ１２２又は暗号化コンテンツ配信サーバ１２４から取得する。コンテンツを復号するための鍵（以下、コンテンツ鍵）及びコンテンツ利用条件は、マルチキャスト配信サーバ１２２、ユニキャスト配信サーバ１２３のいずれかのコンテンツ鍵配信サーバから配信される。コンテンツ鍵がユニキャスト配信されるコンテンツは暗号化コンテンツ配信サーバ１２４に登録され、コンテンツ鍵がマルチキャスト配信されるコンテンツはマルチキャスト配信サーバ１２２に登録

される。

コンテンツ利用条件とは、ユーザがコンテンツを利用する際の制限事項であり、再生可能回数、再生可能期間、再生可能時間等が設定される。クライアント機器１１０は、取得した暗号化コンテンツをコンテンツ鍵で復号し、コンテンツ利用条件に従って再生する。再生可能回数とは、コンテンツを利用する回数の制限であり、コンテンツを利用する度にその回数は減少し、０になると利用できなくなる。再生可能期間とは、コンテンツを利用することのできる期間であり、コンテンツを利用する日時がその期間内であるときのみ利用可能である。再生可能時間とは、コンテンツを利用することができる残り時間であり、コンテンツを利用した時間分、減少し、０になると利用できなくなる。

本システムの構成要素について説明する。

クライアント機器１１０は、ユーザがコンテンツを再生する機器である。また、クライアント機器１１０は、その機器を一意に識別するための識別子であるクライアントＩＤを持つ。クライアントＩＤは工場出荷時に設定され、出荷後はユーザによって変更されることはない。なお、クライアント機器１１０はユニキャスト配信及びマルチキャスト配信による本システムの配信を受けることが可能であることをクライアントＩＤにより確認することができる。

ユーザ管理サーバ１２０は、本システムを用いたコンテンツ配信サービスに加入しているユーザの管理を行う。ユーザ管理サーバ１２０は、ユーザ管理データベース（以下、「ＤＢ」と略記する。）１８０を備える。ユーザ管理ＤＢ１８０では、ユーザを一意に識別するためのユーザＩＤ、ユーザ名、ユーザを認証するためのパスワード、ユーザの使用するクライアント機器１１０のクライアントＩＤなどを保持し管理する。

ユーザ管理ＤＢ１８０で保持し管理するデータの一例を図２に示す。

図２では、ユーザ名“Ｕｓｅｒ１”には、ユーザＩＤ“Ｕｓｅｒ＿１１１１”、パスワード“ａａａｂｂｂｃｃｃ”が設定され、クライアントＩＤ“１２３＿ａｂｃ”のクライアント機器１１０を所有していることを示している。ユーザＩＤはユーザ登録の際、ユーザ管理サーバで割り当てられ、パスワードはユーザ自身が設定する。

コンテンツ配信管理サーバ１２１は、コンテンツホルダからのコンテンツ

配信要求を受け、コンテンツ鍵およびコンテンツ利用条件の配信方式を決定する機能を持つ。また、コンテンツホルダの管理、各コンテンツの配信方式の管理を行う。コンテンツ配信管理サーバ１２１は、コンテンツホルダ管理ＤＢ１４０、コンテンツ配信方式管理ＤＢ１４１、配信方式決定ルールＤＢ１４２を備える。コンテンツホルダ管理ＤＢ１４０では、コンテンツの配信要求を受け付けるコンテンツホルダに関する情報を保持し管理するため、コンテンツホルダを一意に識別するためのコンテンツホルダＩＤ、コンテンツホルダ名、認証のためのパスワードなどを保持する。図３に、コンテンツホルダ管理ＤＢ１４０で保持し管理するデータの一例を示す。

図３では、例えば、コンテンツホルダ名“Ｃ＿ＨＯＬＤＥＲ＿１”には、コンテンツホルダＩＤ“Ｈｏｌｄｅｒ＿１１１１”、パスワード“ａｂｃｒｓｔ”が設定さていることを示している。

コンテンツ配信方式管理ＤＢ１４１では、コンテンツを一意に識別するためのコンテンツＩＤ、コンテンツ名、コンテンツを提供するコンテンツホルダのコンテンツホルダＩＤ、コンテンツの圧縮フォーマット、コンテンツ鍵およびコンテンツ利用条件の配信方式、コンテンツの再生時間、暗号化コンテンツのデータサイズなどを保持し管理する。図４に、コンテンツ配信方式管理ＤＢ１４１で保持及び管理するデータの一例を示す。

図４では、例えば、コンテンツ名“世界の山脈”は、コンテンツＩＤ“ＣＯＮＴ＿０００１”で表され、コンテンツホルダＩＤ“Ｈｏｌｄｅｒ＿１１１１”が所有するコンテンツであり、圧縮フォーマットが“ＭＰＥＧ－２”、配信方式が“ユニキャスト方式”、再生時間“６０分”、データサイズが“１，５００ＭＢ”であることを示している。

配信方式決定ルールＤＢ１４２では、コンテンツに応じて配信方式を決定するためのルールを保持し管理する。配信方式決定ルールＤＢ１４２で保持及び管理するデータの詳細については後述する。

マルチキャスト配信サーバ１２２は、コンテンツ鍵およびコンテンツ利用条件を予め設定された時間にユーザ管理サーバ１２０で管理されているユーザの所有するクライアント機器１１０に対してＩＰマルチキャストにより毎日配信する。マルチキャスト配信サーバ１２２は、配信スケジュールＤＢ１５０およびマルチキャストコンテンツＤＢ１５１を備える。配信スケジュールＤＢ１５０は、コンテンツ鍵をマルチキャストで配信する時間、配信

するコンテンツ鍵で再生可能なコンテンツのコンテンツＩＤ、配信するコンテンツ鍵およびコンテンツ利用条件などを保持し管理する。マルチキャストコンテンツＤＢ１５１は、コンテンツ鍵がマルチキャスト配信により配信されるコンテンツについてのみ、暗号化コンテンツデータを格納する。図５は、配信スケジュールＤＢ１５０で保持し管理する配信スケジュール表の一例を示す図である。

図５（ａ）で示すように、コンテンツＩＤ“ＣＯＮＴ＿０００１”のコンテンツはコンテンツ鍵“０ｘａａａａ... ａａａａ”により暗号化されている。コンテンツＩＤ“ＣＯＮＴ＿０００１”のコンテンツ利用条件には“再生回数３回”という制限が設定されており、“１２：００”にコンテンツ鍵が配信されるように設定されている。この他に、配信スケジュール表には、マルチキャストコンテンツＤＢ１５１内の各コンテンツの格納場所を示すファイルパスなどが記述されている。

ユニキャスト配信サーバ１２３は、ユーザ管理サーバ１２０で管理されているユーザから要求があった場合に、コンテンツ鍵およびコンテンツ利用条件を配信するサーバである。ユニキャスト配信サーバ１２３は、配信データ管理ＤＢ１６０を備える。配信データ管理ＤＢ１６０では、配信するコンテンツ鍵で再生可能なコンテンツのコンテンツＩＤ、配信するコンテンツ鍵およびコンテンツ利用条件を保持し管理する。配信データ管理ＤＢ１６０で管理するデータの一例を図６に示す。図６では、コンテンツＩＤ“ＣＯＮＴ＿０００１”のコンテンツはコンテンツ鍵“０ｘ１１１１... １１１１”により暗号化されている。コンテンツＩＤ“ＣＯＮＴ＿０００１”のコンテンツ利用条件には“再生回数３回”という制限設定されていることを示している。

暗号化コンテンツ配信サーバ１２４は、ユーザが暗号化コンテンツをダウンロードするためのサーバである。暗号化コンテンツ配信サーバ１２４は、暗号化コンテンツ管理ＤＢ１７０およびユニキャストコンテンツＤＢ１７１を備える。暗号化コンテンツ管理ＤＢ１７０では、コンテンツＩＤ、暗号化コンテンツのデータサイズおよび暗号化されたコンテンツデータが格納されているファイルパスなどを保持し管理する。ユニキャストコンテンツＤＢ１７１は、コンテンツ鍵がユニキャストにより配信されるコンテンツについて、暗号化コンテンツデータを格納する。図７に、暗号化コンテンツ管理ＤＢ１７０で保持及び管理するデータの一例を示す。図７では、コンテンツ

ＩＤ“ＣＯＮＴ＿０００１”の暗号化コンテンツデータのサイズは“１，５００ＭＢ”であり、コンテンツ鍵の配信方式はユニキャスト配信であり、暗号化コンテンツデータはユニキャストコンテンツＤＢ１７１の“Ｃ：￥ｃｏｎｔｅｎｔ￥ｃｏｎｔ＿０００１．ｅｎｃ”に格納されていることを示している。

図８（ａ）および図８（ｂ）に、マルチキャストコンテンツＤＢ１５１に格納される暗号化コンテンツとユニキャストコンテンツＤＢ１７１に格納される暗号化コンテンツとのデータ構造の相違を示す。図８（ａ）は、図１に示したユニキャストコンテンツＤＢ１７１に格納される暗号化コンテンツのデータ構造を示す図である。図８（ｂ）は、図１に示したマルチキャストコンテンツＤＢ１５１に格納される暗号化コンテンツのデータ構造を示す図である。図８（ａ）に示すように、コンテンツ鍵がユニキャストで配信されるコンテンツは、コンテンツＩＤと暗号化コンテンツデータとから構成されている。これに対し、コンテンツ鍵がマルチキャスト配信されるコンテンツは、図８（ｂ）に示すように、コンテンツＩＤ、コンテンツ鍵、コンテンツ利用条件および暗号化コンテンツデータなどから構成されている。すなわち、図８（ａ）のコンテンツに、さらに、コンテンツ鍵およびコンテンツ利用条件が重畳されている。コンテンツ鍵及びコンテンツ利用条件の部分のデータについては、特定のクライアント機器１１０のみ利用可能とするため、受信データを利用できるクライアント機器１１０を限定する機能を用いて保護されているものとする。具体的には、コンテンツに重畳され、マルチキャストされるコンテンツ鍵及びコンテンツ利用条件は、あらかじめ暗号化されているものとする。暗号化されたコンテンツ鍵及びコンテンツ利用条件を復号するための復号鍵は、ユーザ登録したユーザにのみ配布される。この復号鍵の配布方法には、あらかじめ復号鍵がＲＯＭ（Read Only Memory）などの不揮発性メモリに書き込まれたクライアント機器１１０をユーザ登録したユーザに配布する方法や、この復号鍵が記録された記録媒体をユーザ登録したユーザに配布する方法などがある。これにより、ユーザ登録をしたユーザのクライアント機器１１０は、ＲＯＭや配布された記録媒体などから復号鍵を読み出して、マルチキャストされたコンテンツに重畳されているコンテンツ鍵及びコンテンツ利用条件を復号することができる。この復号されたコンテンツ鍵を用いて、当該クライアント機器１１０は、暗号化コンテン

ツを復号し、その後、復号されたコンテンツ利用条件に従ってコンテンツを利用することができる。なお、暗号化されたコンテンツ鍵を復号するための復号鍵は、必ずしもＲＯＭや記録媒体に記録されて配布される必要はなく、ユーザ登録をしたユーザに、あらかじめセキュアな通信により配布されていればよい。この暗号化方法については、非特許文献：中野他、“デジタルコンテンツ保護用鍵管理方式”、２００１年暗号と情報セキュリティシンポジウム講演論文集、５Ａ－５、２００１に詳しい。なお、マルチキャストされるコンテンツ鍵及びコンテンツ利用条件を、ユーザ登録したユーザにだけ利用できるようにする方法は、デジタルコンテンツ保護用鍵管理方式に限定されず、他の方法であってもよい。このようなデータ構造を持つ暗号化コンテンツは、コンテンツ配信管理サーバ１２１によって生成され、マルチキャストコンテンツＤＢ１５１に格納されてもよいし、マルチキャスト配信サーバ１２２によって生成され、マルチキャストコンテンツＤＢ１５１に格納されてもよい。

コンテンツ登録用端末１００は、コンテンツホルダがコンテンツ配信管理サーバ１２１に配信するコンテンツの登録を行う際に用いる端末である。コンテンツの登録については後述する。

以下、サービス内の各処理について、コンテンツホルダによる配信コンテンツの登録、配信方式の決定方法、ユーザによるユーザ登録、ユーザのコンテンツ利用について順に説明する。

まず、コンテンツホルダによる配信コンテンツの登録について説明する。

コンテンツホルダは、コンテンツ配信管理サーバ１２１に対し、コンテンツ登録用端末１００を用いてコンテンツ登録要求を行う。図９にコンテンツホルダによるコンテンツ登録処理のフローチャートを示す。

コンテンツ配信管理サーバ１２１は、コンテンツホルダからの配信コンテンツの登録要求を受ける前に、コンテンツホルダの認証を行う。本実施の形態においては、コンテンツホルダは事前にコンテンツホルダ管理ＤＢ１４０に登録されている必要がある。コンテンツホルダは、配信コンテンツ登録要求時にコンテンツ登録用端末１００を用いて、通信路１３０を介しコンテンツ配信管理サーバ１２１へコンテンツホルダＩＤとパスワードを送信する。コンテンツ配信管理サーバ１２１は受信したコンテンツホルダＩＤとパスワードの組をコンテンツホルダ管理ＤＢ１４０に登録されているデータと

照会することでログインの成否を判定する（Ｓ９０１）。

コンテンツホルダはコンテンツ配信管理サーバ１２１でのログインが成功した後（Ｓ９０２）、コンテンツ配信管理サーバ１２１に対し、配信するコンテンツの登録要求を送る（Ｓ９０３）。この際、コンテンツホルダは、暗号化コンテンツ、コンテンツ鍵、コンテンツ利用条件、コンテンツメタデータを送信する。本実施の形態では、コンテンツの圧縮フォーマットはＭＰＥＧ－２であり、コンテンツは１２８ビットの鍵を用いてＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）で暗号化されている。ＭＰＥＧ－２についてはＩＳＯ／ＩＥＣ　１３８１８、ＡＥＳについてはＦＩＰＳ－１９７に詳しい。

メタデータにはコンテンツを一意に識別する「コンテンツＩＤ」、「コンテンツ名」、「コンテンツホルダ名」、コンテンツの「圧縮フォーマット」、「再生時間」、「暗号化コンテンツのデータサイズ」が記述されている。図１０にメタデータの一例を示す。図１０では、コンテンツＩＤ“ＣＯＮＴ＿０００１”のコンテンツのコンテンツ名は“世界の山脈”であり、このコンテンツを提供したコンテンツホルダは“コンテンツホルダ＿ＡＢＣ”である。圧縮フォーマットは“ＭＰＥＧ－２”であり、再生時間は“６０分”、暗号化コンテンツのデータサイズは“１，５００ＭＢ”である。なお、メタデータには、他に「製作年度」、圧縮率「ＣＢＲ（Constant Bit Rate）、およびＶＢＲ（Variable Bit Rate）の平均レート」等が含まれても構わない。

コンテンツ配信管理サーバ１２１は、コンテンツホルダからコンテンツ登録要求で受け取ったメタデータ中のコンテンツ圧縮フォーマットと配信方式決定ルールＤＢ１４２とから登録するコンテンツ鍵の配信方式を決定する（Ｓ９０４）。コンテンツ鍵の配信方式決定方法については後述する。

ユニキャスト配信と決定された場合（Ｓ９０５）、コンテンツ配信管理サーバ１２１はコンテンツ鍵、コンテンツ利用条件、メタデータ、及びコンテンツ配信条件をユニキャスト配信サーバ１２３へ登録する（Ｓ９０６）。併せて、コンテンツ配信管理サーバ１２１は、その暗号化コンテンツデータを暗号化コンテンツ配信サーバ１２４に登録する。ユニキャスト配信サーバ１２３が持つ配信データ管理ＤＢ１６０で保持及び管理するデータは図６にあるデータを用いる。

マルチキャスト配信と決定された場合（Ｓ９０５）、コンテンツ配信管理

サーバ１２１はコンテンツ鍵、コンテンツ利用条件、メタデータ及び暗号化コンテンツデータをマルチキャスト配信サーバ１２２へ登録する（Ｓ９０７）。マルチキャスト配信サーバ１２２では、新たに登録された暗号化コンテンツデータをマルチキャストコンテンツＤＢ１５１に格納し、配信スケジュールの空いている時間に新たに登録されたコンテンツの配信スケジュールを追加し、配信スケジュールＤＢ１５０を更新する。

図５に配信スケジュールＤＢ１５０の更新の様子を示す。図５（ａ）に示すように、更新前の配信スケジュールＤＢ１５０に対し、コンテンツＩＤ“ＣＯＮＴ＿０００２”、コンテンツ鍵“０ｘｂｂｂｂ・・・ｂｂｂ（１２８ｂｉｔ）”、コンテンツ利用条件“再生回数１回”のコンテンツの配信スケジュールを追加する場合を考える。更新前には“１３：００”の配信スケジュールが空いているため、その時間を、追加するコンテンツの配信スケジュールとして設定し、配信スケジュールＤＢ１５０を更新すると、図５（ｂ）に示す更新後の配信スケジュールＤＢの状態になる。

コンテンツ配信管理サーバ１２１は、決定した配信方式に従って各配信サーバにコンテンツ鍵、コンテンツ利用条件を登録後、コンテンツ鍵がユニキャスト配信される暗号化コンテンツを暗号化コンテンツ配信サーバ１２４へ登録し（Ｓ９０８）、処理を終了する。

次に、図９に示したＳ９０４のコンテンツ鍵の配信方式の決定方法の処理の詳細について図１１を用いて説明する。

コンテンツ配信管理サーバ１２１はコンテンツホルダからコンテンツメタデータを受信した後、コンテンツ鍵及びコンテンツ利用条件の配信方式を決定する。具体的には、まず、コンテンツ配信管理サーバ１２１はコンテンツ鍵配信方式決定ルールを、配信方式決定ルールＤＢ１４２より取得する（Ｓ１００１）。

本実施の形態では、コンテンツの圧縮フォーマットによって、コンテンツを利用するユーザ数が変わることを想定し、コンテンツのメタデータ中に記述されるコンテンツ圧縮フォーマットを、コンテンツ鍵及びコンテンツ利用条件の配信方式決定のためのパラメータとする。

図１２（ａ）に、本実施の形態の配信方式決定ルールＤＢ１４２で保持し管理するデータ（配信方式決定ルール）の一例を示す。このルールでは、登録するコンテンツのメタデータ中にある圧縮フォーマットを配信方式決定

のパラメータとしている。そのパラメータを用いて、配信方式決定ルールに従って配信方式を決定する（Ｓ１００２）。この場合、圧縮フォーマットがＭＰＥＧ－２、又はＡＶＩ（Audio、Video、 still Images）の場合にはユニキャスト配信、ＭＰＥＧ－４の場合にはマルチキャスト配信を選択するように設定されている。ＭＰＥＧ－４についてはＩＳＯ／ＩＥＣ　１４４９６に詳しい。

以下、上記配信方式決定ルールＤＢ１４２で管理されるデータ（配信方式決定ルール）の他の例について説明する。

図１２（ｂ）に、コンテンツホルダに応じて配信方式を変更するような要求があることを想定し、コンテンツ配信方式を決定するパラメータをコンテンツホルダＩＤにした場合の配信方式決定ルールの一例を示す。コンテンツホルダＩＤ“Ｈｏｌｄｅｒ＿１１１１”および“Ｈｏｌｄｅｒ＿３３３３”の場合にはユニキャスト配信、コンテンツホルダＩＤ“Ｈｏｌｄｅｒ＿２２２２”の場合にはマルチキャスト配信を選択するように設定されている。

図１２（ｃ）に、コンテンツの画質によりコンテンツを利用するユーザ数が変わることを想定し、コンテンツ配信方式を決定するパラメータをＣＢＲおよびＶＢＲの平均レートにした場合の配信方式決定ルールの一例を示す。ここでは、ＣＢＲおよびＶＢＲの平均レートが５００ｋｂｐｓ未満の場合にはマルチキャスト配信、５００ｋｂｐｓ以上１５Ｍｂｐｓ未満の場合、および１５Ｍｂｐｓ以上の場合にはユニキャスト配信をそれぞれ選択するように設定されている。

図１２（ｄ）に、コンテンツが最初に配信されてからの経過時間により配信方式を変更する要求があることを想定し、コンテンツ配信方式を決定するパラメータをコンテンツ利用条件にした場合の配信方式決定ルールの一例を示す。コンテンツ利用条件が、“再生回数　３回”の場合および“再生期間　２００３／０１／０１～２００３／０１／３１”の場合にはユニキャスト配信、“再生回数　制限無し”および“再生期間　２００３／０２／０１～２００３／０２／２８”の場合にはマルチキャスト配信をそれぞれ選択するよう設定されている。

次にユーザ登録の動作について図１３を用いて説明する。

ユーザはコンテンツを利用する際、ユーザ管理サーバ１２０に事前にユーザ登録しておく。より具体的には、まず、ユーザはクライアント機器１１０

を用いて、ユーザ管理サーバ１２０に対し、登録要求を行う。次いで、ユーザ名、パスワード、及びユーザが利用するクライアント機器１１０のクライアントＩＤをユーザ管理サーバへ送信する（Ｓ１２０１）。ただし、クライアント機器１１０のクライアントＩＤは、ユーザがユーザ名およびパスワードとともに手入力してもよいが、ユーザが入力したユーザ名およびパスワードにクライアント機器１１０がクライアントＩＤを自動的に添付して送信するのが一般的である。ユーザの登録要求を受けたユーザ管理サーバ１２０では、ユーザＩＤを割り当て（Ｓ１２０２）、ユーザ管理ＤＢ１８０へのデータ追加（Ｓ１２０３）を行い、ユーザ登録終了をクライアント機器１１０へ通知して終了する。

次にユーザのコンテンツ利用の動作について図１４を用いて説明する。

コンテンツ利用のサービスは、ユーザ登録したユーザにのみ提供されるものであり、一旦ユーザ管理サーバ１２０で認証をする必要がある。そのため、認証に必要なデータの送受信がクライアント機器１１０とユーザ管理サーバ１２０との間で行われる（Ｓ１３０１）。クライアント機器１１０は認証の成否を判定し、認証が成功した場合のみ、以降の処理を行うことができる（Ｓ１３０２）。

ユーザは、コンテンツを利用する際、コンテンツ配信管理サーバ１２１から、現在配信を行っているコンテンツに関する情報を取得する（Ｓ１３０３）。

コンテンツに関する情報には、図４のように、コンテンツＩＤ、コンテンツ名、コンテンツを提供するコンテンツホルダ名（又はコンテンツホルダＩＤ）、圧縮フォーマット、コンテンツ鍵の配信方式、コンテンツの再生時間、暗号化コンテンツのデータサイズなどが含まれている。クライアント機器１１０は、コンテンツ配信管理サーバ１２１から取得したコンテンツに関する情報に基づいて、コンテンツの配信を要求するためのコンテンツリストを生成し、ユーザに表示する。

ユーザはコンテンツリストから利用したいコンテンツを選択する（Ｓ１３０４）。クライアント機器１１０は、コンテンツリストから選択されたコンテンツの配信要求を暗号化コンテンツ配信サーバ１２４に送信する。暗号化コンテンツ配信サーバ１２４は、配信要求されたコンテンツのコンテンツ鍵がユニキャスト配信される場合にのみ、暗号化されたコンテンツを配信する。クライアント機器１１０は、暗号化コンテンツ配信サーバ１２４から暗号化

コンテンツを取得できた場合、コンテンツ鍵の配信方式がユニキャスト配信であると判定する（Ｓ１３０５）。一方、暗号化コンテンツ配信サーバ１２４から暗号化コンテンツを取得できなかった場合、クライアント機器１１０は、コンテンツ鍵の配信方式がマルチキャスト配信であると判定する。

以下、選択されたコンテンツのコンテンツ鍵、及びコンテンツ利用条件の配信方式別に説明する。

選択したコンテンツのコンテンツ鍵、及びコンテンツ利用条件がユニキャスト配信の場合について説明する。選択されたコンテンツのコンテンツ鍵がユニキャスト配信で配信されていると判定した場合、クライアント機器１１０は、さらに、選択されたコンテンツのコンテンツ鍵をクライアント機器１１０の内部に保持しているか否かを調べる（Ｓ１３０６）。選択されたコンテンツのコンテンツ鍵をクライアント機器１１０がすでに保持している場合は、保持しているコンテンツ鍵を用いてクライアント機器１１０での再生処理を行う（Ｓ１３１１）。選択されたコンテンツのコンテンツ鍵をクライアント機器１１０が保持していない場合、ユーザのクライアント機器１１０とユニキャスト配信サーバ１２４との間で認証を行い、秘匿性・耐改竄性が保証された通信を行う（Ｓ１３０７）。このような通信方式について本実施の形態では特に手法を記述しないが、ＳＳＬ（Ｓｅｃｕｒｅ Ｓｏｃｋｅｔｓ Ｌａｙｅｒ）等を用いる。ＳＳＬについては、Ａ．Ｆｒｉｅｒ他、“Ｔｈｅ ＳＳＬ ３．０ Ｐｒｏｔｏｃｏｌ”、Ｎｅｔｓｃａｐｅ Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ Ｃｏｒｐ．Ｎｏｖ．１８、１９９６に詳しい。なお、クライアント機器１１０とユニキャスト配信サーバ１２３との間で認証はＰＫＩ方式や共通鍵方式による認証でも構わない。前述の通信によって、クライアント機器１１０はコンテンツ鍵及びコンテンツ利用条件をユニキャスト配信サーバ１２３から取得する（Ｓ１３０８）。ステップＳ１３０７において、ユニキャスト配信サーバ１２３との認証に失敗した場合、クライアント機器１１０は処理を終了する。

選択されたコンテンツのコンテンツ鍵、及びコンテンツ利用条件がマルチキャスト配信の場合について説明する。選択されたコンテンツのコンテンツ鍵がマルチキャスト配信で配信されていると判定した場合、クライアント機器１１０は、選択されたコンテンツのコンテンツ鍵をクライアント機器１１０の内部に保持しているか否かを調べる（Ｓ１３０９）。選択されたコンテ

ンツのコンテンツ鍵をクライアント機器１１０がすでに保持している場合は、保持しているコンテンツ鍵を用いてクライアント機器１１０での再生処理を行う（Ｓ１３１１）。選択されたコンテンツのコンテンツ鍵をクライアント機器１１０が保持していない場合、クライアント機器１１０は、マルチキャスト配信サーバ１２２からコンテンツ鍵の配信を受ける。マルチキャスト配信の場合、マルチキャスト配信サーバ１２２は予め設定された配信スケジュールに基づき、コンテンツ、コンテンツ鍵及びコンテンツ利用条件をマルチキャストする。クライアント機器１１０はコンテンツ鍵及びコンテンツ利用条件がクライアント機器１１０内に保持されていないため、次のマルチキャストによる配信まで待機する（Ｓ１３１０）。マルチキャスト配信のスケジュールについては、クライアント機器１１０はマルチキャスト配信サーバ１２２から取得することが可能である。本実施の形態でのマルチキャストによる配信方式は、ユーザ管理サーバ１２０で管理されているユーザの利用するクライアント機器１１０にのみ配信する必要があるため、受信データを利用できるクライアント機器１１０を限定する機能を備えた配信方式で実現する。具体的実現方法については、非特許文献：中野他、“デジタルコンテンツ保護用鍵管理方式、”２００１年暗号と情報セキュリティシンポジウム講演論文集、５Ａ－５、２００１に詳しい。

各配信処理ともに、コンテンツ、コンテンツ鍵、及びコンテンツ利用条件を取得した後、クライアント機器１１０内部での再生処理が行われる（Ｓ１３１１）。

次に、図１４のステップＳ１３１１におけるクライアント機器１１０内部での再生処理の詳細について、図１５、及び図１６を用いて説明する。図１５は、クライアント機器１１０の構成を示す機能ブロック図である。図１６は、図１４のステップＳ１３１１におけるクライアント機器１１０内部でのコンテンツ再生処理の動作を示すフローチャートである。

クライアント機器１１０は、通信部１４０１、利用条件判定部１４０２、暗号化コンテンツ蓄積部１４０３、コンテンツ復号部１４０４、コンテンツデコード部１４０５、クライアントＩＤ蓄積部１４０６、コンテンツ鍵蓄積部１４０７、入力部１４０８、要求処理部１４０９、配信方式判定部１４１０および画面出力部１４１１を備える。

通信部１４０１は、各種サーバと通信するための機能処理部である。利用

条件判定部１４０２は、コンテンツの新たな利用がコンテンツ利用条件を満たしているかを判定する機能処理部である。暗号化コンテンツ蓄積部１４０３は、暗号化コンテンツを蓄積する記憶部および機能処理部である。図１４のステップＳ１３０５またはステップＳ１３０８で取得された暗号化コンテンツは、暗号化コンテンツ蓄積部１４０３に蓄積される。コンテンツ復号部１４０４は、コンテンツ鍵を用いて暗号化コンテンツの復号を行う機能処理部である。

コンテンツデコード部１４０５は、コンテンツの圧縮フォーマットに応じてコンテンツをデコードし、映像および音声データを出力する機能処理部である。クライアントＩＤ蓄積部１４０６は、クライアントＩＤを蓄積する記憶部および機能処理部であり、サーバとの通信においてクライアントＩＤの送信が必要なとき、通信部１４０１はここからクライアントＩＤを取得する。コンテンツ鍵蓄積部１４０７は、コンテンツ鍵及びコンテンツ利用条件を蓄積する記憶部および機能処理部である。図１４のステップＳ１３０８で取得されたコンテンツ鍵およびコンテンツ利用条件は、コンテンツ鍵蓄積部１４０７に蓄積される。入力部１４０８はユーザからの要求を入力する機能処理部である。要求処理部１４０９は、入力部１４０８より入力された要求に応じて処理を行う機能処理部である。配信方式判定部１４１０は、ユーザによって選択されたコンテンツのコンテンツ鍵が、マルチキャストで配信されるか、ユニキャストで配信されるかのいずれであるかを判定する。画面出力部１４１１は再生する動画やサーバからの情報を描画し、ユーザに提示する機能処理部である。

クライアント機器１１０は、コンテンツ鍵蓄積部１４０７に格納されているコンテンツ鍵、およびコンテンツ利用条件を取得した後、利用条件判定部１４０２にて、現在時刻におけるコンテンツの新たな利用が、取得されたコンテンツ利用条件に示される条件を満たしているか確認をする（Ｓ１５０１）。例えば、再生可能回数が０でないかの確認や、コンテンツを再生する日時が再生可能期間内であるかの確認である。コンテンツ利用条件が満足されている場合、利用条件判定部１４０２はコンテンツ鍵蓄積部１４０７に格納されているコンテンツ鍵をコンテンツ復号部１４０４へ送信する（Ｓ１５０１）。コンテンツ復号部１４０４は、暗号化コンテンツ蓄積部１４０３より当該暗号化コンテンツを取得し、利用条件判定部１４０２より取得したコ

ンテンツ鍵を用いて復号する（Ｓ１５０２）。復号化されたデータをコンテンツデコード部１４０５へ送信する。コンテンツデコード部１４０５は、圧縮フォーマットに応じてコンテンツをデコードし、映像および音声データを出力し（Ｓ１５０３）、処理を終了する。

以上のように、本実施の形態のコンテンツ配信システム２００によれば、コンテンツ及びコンテンツ鍵などを配信する側では、各コンテンツの属性に応じて、コンテンツ鍵及びコンテンツ利用条件の配信方式を切り替えて配信することができる。これにより、例えば、同一のコンテンツに対し、コンテンツ鍵及びコンテンツ利用条件の配信要求が殺到することが予測される場合には、そのコンテンツ鍵及びコンテンツ利用条件をマルチキャストによって配信し、コンテンツ配信システム２００内のサーバ負荷を低減することができる。また、コンテンツの著作権保護の方が、コンテンツ配信システム２００のサーバ負荷よりも優先される場合には、コンテンツ鍵及びコンテンツ利用条件をユニキャストによって配信し、著作権の安全性を向上することができる。また、クライアント機器１１０側では、内部の配信方式判定部１４１０でコンテンツ鍵及びコンテンツ利用条件の配信方式を判定することができるので、コンテンツ毎に異なる配信方式で配信されるコンテンツ鍵及びコンテンツ利用条件を、支障なく取得することができる。これによって、何ら問題なく所望のコンテンツを利用することができる。

なお、コンテンツ配信管理サーバ１２１、マルチキャスト配信サーバ１２２、ユニキャスト配信サーバ１２３、暗号化コンテンツ配信サーバ１２４、ユーザ管理サーバ１２０は独立でなく、一つのサーバが別のサーバの機能を兼ねてもよい。

なお、マルチキャストによる配信は毎日行われなくてもよい。

なお、コンテンツ鍵の配信方式を決定するパラメータは、コンテンツの圧縮フォーマット以外に、コンテンツホルダＩＤ、ＣＢＲおよびＶＢＲの平均レート、コンテンツ利用条件などでも構わない。

また、コンテンツ鍵の配信方式を決定するパラメータをいずれにするかは、コンテンツホルダがコンテンツを登録する際に、コンテンツ配信管理サーバ１２１に指定してもよいし、コンテンツ配信管理サーバ１２１がコンテンツ配信システム２００における各サーバの負荷に応じて動的に決定するとしてもよい。

なお、暗号化コンテンツの取得方法としては、メディアによる配信、放送などのブロードキャストによる配信でも構わない。

なお、上記実施の形態では、クライアント機器１１０は、所望のコンテンツの配信を暗号化コンテンツ配信サーバ１２４に要求することによって、コンテンツ鍵の配信方式を判定した。すなわち、マルチキャストで配信されるコンテンツ鍵およびコンテンツ利用条件はコンテンツに重畳されており、マルチキャスト配信サーバ１２２のみから配信されたが、本発明はこれに限定されない。例えば、クライアント機器１１０は、コンテンツに重畳されている情報を読み取ることによって、コンテンツ鍵の配信方式を判定するとしてもよい。すなわち、コンテンツには、コンテンツ鍵およびコンテンツ利用条件の実体の代わりに、コンテンツ鍵およびコンテンツ利用条件の配信方式を示す情報が重畳されているとしてもよい。図１７は、コンテンツ鍵の配信方式を示す情報が暗号化コンテンツデータに重畳されている場合におけるコンテンツのデータ構造の一例を示す図である。同図のように、暗号化コンテンツデータには、コンテンツＩＤおよびコンテンツ鍵及びコンテンツ利用条件の配信方式を示す情報が重畳される。

この場合、コンテンツ配信管理サーバ１２１は、各コンテンツのコンテンツ鍵およびコンテンツ利用条件の配信方式を決定した後、決定された配信方式を示す情報を各コンテンツに重畳し、暗号化コンテンツ配信サーバ１２４に登録する。従って、コンテンツは、コンテンツ鍵およびコンテンツ利用条件の配信方式にかかわらず、暗号化コンテンツ配信サーバ１２４から一元的に配信される。また、コンテンツ配信管理サーバ１２１は、各コンテンツのコンテンツ鍵およびコンテンツ利用条件の配信方式を決定した後、コンテンツ鍵およびコンテンツ利用条件を、決定された配信方式に従って、ユニキャスト配信サーバ１２３およびマルチキャスト配信サーバ１２２に登録する。

これに対応して、クライアント機器１１０では、ユーザがコンテンツを利用しようとする際に、まず、暗号化コンテンツ配信サーバ１２４から暗号化コンテンツを取得する。その後、配信方式判定部１４１０は、取得された暗号化コンテンツに重畳されている情報から、コンテンツ鍵及びコンテンツ利用条件の配信方式を判定し、判定結果に従って、対応するサーバからコンテンツ鍵及びコンテンツ利用条件を取得する。すなわち、コンテンツ鍵及びコンテンツ利用条件の配信方式がマルチキャストであると判定した場合には、

マルチキャスト配信サーバ１２２からコンテンツ鍵及びコンテンツ利用条件が配信されるのを待機し、コンテンツ鍵及びコンテンツ利用条件の配信方式がユニキャストであると判定した場合には、ユニキャスト配信サーバ１２３にコンテンツ鍵及びコンテンツ利用条件の配信を要求する。以下、クライアント機器１１０におけるコンテンツの再生処理は、図１６を用いてすでに説明したとおりである。

さらに、クライアント機器１１０は、コンテンツ鍵およびコンテンツ利用条件の配信方式を特定するための情報を、サーバから取得するとしてもよい。具体的には、クライアント機器１１０は、図１４に示したステップＳ１３０３の処理において、コンテンツ配信管理サーバ１２１に対し、コンテンツに関する情報を要求する。コンテンツ配信管理サーバ１２１はクライアント機器１１０の要求に応じ、コンテンツ配信方式管理ＤＢ１４１から図４に示したデータ（コンテンツに関する情報）を読み出して、クライアント機器１１０に送信する。クライアント機器１１０は、コンテンツ配信管理サーバ１２１から取得したコンテンツに関する情報を参照して、コンテンツ鍵の配信方式を判定し、判定された配信方式に応じたサーバからコンテンツ鍵及びコンテンツ利用条件を取得する。

この方法によれば、クライアント機器１１０は、コンテンツをコンテンツ鍵およびコンテンツ利用条件よりも先に取得しておく必要はなく、コンテンツ鍵およびコンテンツ利用条件を取得した後にコンテンツを取得しても、問題なくコンテンツを利用することができる。

なお、暗号化コンテンツは、コンテンツ鍵の配信方式にかかわらず、すべて図８（ａ）に示したデータ構造とし、暗号化コンテンツ配信サーバ１２４が一元的に管理し配信するとしてもよい。もちろん、上記実施の形態と同様に、コンテンツ鍵がユニキャストで配信されるコンテンツのみ図８（ａ）に示したデータ構造で、暗号化コンテンツ配信サーバ１２４から配信され、コンテンツ鍵がマルチキャストで配信されるコンテンツは図８（ｂ）に示したデータ構造で、マルチキャスト配信サーバ１２２から配信されるとしてもよい。また、ユニキャスト配信サーバ１２３の負荷が大きくなるが、暗号化コンテンツ配信サーバ１２４をなくして、その代わりにユニキャスト配信サーバ１２３もマルチキャスト配信サーバ１２２も、図８（ｂ）に示したデータ構造のコンテンツを配信するとしてもよい。

なお、コンテンツ配信管理サーバ１２１は、クライアント機器１１０の要求に対して、図４に示したようにリストになったコンテンツに関する情報をそのまま送信するのでなくてもよい。例えば、クライアント機器１１０は、利用しようとするコンテンツ毎に、コンテンツ鍵およびコンテンツ利用条件の配信方式を問い合わせるとしてもよい。これに対し、コンテンツ配信管理サーバ１２１は、問い合わせのあったコンテンツについてのみ、コンテンツ鍵及びコンテンツ利用条件の配信方式を回答するとしてもよい。このようにすれば、コンテンツ配信管理サーバ１２１の処理負荷が大きくなるが、クライアント機器１１０において配信方式を判定するための処理負荷が小さくなる。

さらに、コンテンツ配信管理サーバ１２１がクライアント機器１１０の要求に応答してコンテンツに関する情報を送信する代わりに、コンテンツに関する情報を放送やマルチキャストなどにより、あらかじめクライアント機器１１０に配布しておくとしてもよい。

本発明のクライアント機器は、通信機能を備えるコンテンツ再生装置、パーソナルコンピュータ、ＰＤＡ（Personal Digital Assistant)、携帯電話機、ＳＴＢ（Set Top Box）などとして有用である。